PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-025427
(43)Date of publication of application : 27.01.2005

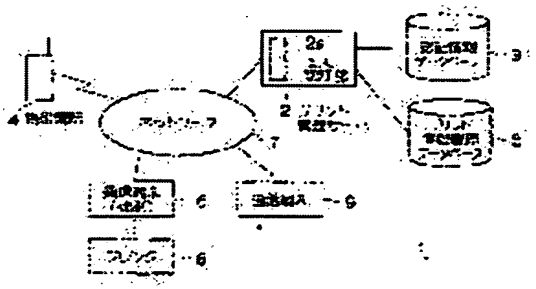
(51)Int.CI. G06F 15/00
G06F 3/12
G06F 13/00

(21)Application number : 2003-189238
(22)Date of filing : 01.07.2003

(71)Applicant : TOSHIBA CORP
TOSHIBA TEC CORP
(72)Inventor : KOYAMA SATOSHI

(54) AUTHENTICATION DEVICE AND SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an authentication device and an authentication system releasing locked personal identification information with simple and greatly ensured security.
SOLUTION: This authentication device is provided with a personal information storage means storing individual personal identification information associated with electronic mail addresses of respective registered users, a personal identity authentication means authenticating the personal identity of the registered user, and a lock releasing information creation means creating lock releasing information releasing prohibition individually when the use of the personal identification information is prohibited. The authentication device is also provided with an electronic mail communication means which transmits a lock notification mail carrying a communication address of the lock releasing information and lock releasing identification information at least to the electronic mail address matching the personal identification information, and a lock releasing means receiving access to the communication address of the lock releasing information and performing authentication based on the received lock releasing identification information for releasing the prohibition of the disabled personal identification information.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-25427
(P2005-25427A)
(43)公開日　平成17年1月27日(2005.1.27)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 15/00	G06F 15/00	330B	5B021
G06F 3/12	G06F 3/12	K	5B085
G06F 13/00	G06F 13/00	547V	
	G06F 13/00	630A	

審査請求 未請求　請求項の数 7　OL　（全 14 頁）

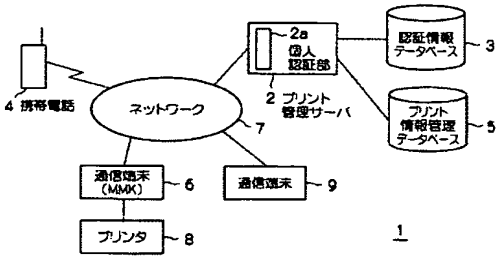
(21)出願番号　特願2003-189238(P2003-189238)
(22)出願日　平成15年7月1日(2003.7.1)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(71)出願人　000003562
東芝テック株式会社
東京都千代田区神田錦町１丁目１番地
(74)代理人　100090620
弁理士　工藤　宜幸
(74)代理人　100092576
弁理士　鎌田　久男
(72)発明者　小山　悟史
東京都港区芝公園２丁目４番１号　秀和芝パークビル　東芝テック株式会社内

Fターム(参考)　5B021 BB00　NN18
5B085 AE01

(54)【発明の名称】認証装置及び認証システム

(57)【要約】
【課題】ロックされた個人識別情報の解除を簡便かつ高いセキュリティで行なう認証装置及び認証システムを提供する。
【解決手段】本発明の認証装置は、登録ユーザの各個人識別情報に少なくとも各登録ユーザの電子メールアドレスを対応付けて記憶する個人情報記憶手段と、登録ユーザの個人認証を行なう個人認証手段と、個人識別情報が使用禁止とされたときに、その禁止を個別に解除するロック解除情報を作成するロック解除情報作成手段と、その個人識別情報に対応する電子メールアドレスを送信先とし、少なくともロック解除情報の通信アドレスとロック解除用識別情報とを記載したロック通知メールを送信する電子メール通信手段と、ロック解除情報の通信アドレスにアクセスを受け、受信したロック解除用識別情報に基づいて認証を行ない、使用禁止された個人識別情報の禁止を解除するロック解除手段とを備える。
【選択図】　図１



【特許請求の範囲】
【請求項１】
登録ユーザの各個人識別情報に、少なくとも各登録ユーザのユーザ通信端末の電子メールアドレスを対応付けた個人情報を記憶する個人情報記憶手段と、
登録ユーザの個人認証を行なう個人認証手段と、
上記個人認証手段により個人認証の正当性が認められず、個人識別情報が使用禁止とされたときに、当該個人識別情報の禁止を個別に解除するロック解除情報を作成するロック解除情報作成手段と、
使用禁止となった上記個人識別情報に対応する電子メールアドレスを送信先とし、少なくとも、上記ロック解除情報に割り当てた通信アドレスと、ロック解除用識別情報とを記載したロック通知メールを送信する電子メール通信手段と、
上記ロック解除情報に割り当てた通信アドレスにアクセスを受け、受信したロック解除用識別情報に基づいて認証を行ない正当である場合、使用禁止された上記個人識別情報の禁止を解除するロック解除手段と
を備えることを特徴とする認証装置。
【請求項２】
上記ロック解除情報作成手段は、上記ロック解除情報の通信アドレスが同時期に重複しない通信先アドレスを割り当てることを特徴とする請求項１に記載の認証装置。
【請求項３】
上記個人認証手段は、
各個人識別情報毎に使用禁止となったロック回数を監視するロック回数監視部と、
所定の監視期間内に所定回数以上のロックがあった個人識別情報とは異なる新しい個人識別情報の作成をする個人識別情報作成手段と、
上記ロック解除手段による解除後、既に登録されている個人識別情報を上記新しい個人識別情報に変更する個人識別情報変更部と
を有することを特徴とする請求項１又は２に記載の認証装置。
【請求項４】
上記ロック解除手段は、上記ロック解除情報の通信先アドレスへのアクセス待ち受け期間を設け、その待ち受け期間までにアクセスがない場合、上記ロック解除情報を無効にすることを特徴とする請求項１～３のいずれかに記載の認証装置。
【請求項５】
上記ロック解除用識別情報が、上記個人認証情報記憶手段に記憶されている個人識別情報及び上記ユーザのみが知るパスワードであることを特徴とする請求項１～４のいずれかに記載の認証装置。
【請求項６】
上記電子メール通信手段は、上記ロック解除手段による解除後、当該個人識別情報に対応する電子メールアドレスを送信先として、ロック解除が終了した旨のロック解除通知メールを送信することを特徴とする請求項１～５のいずれかに記載の認証装置。
【請求項７】
少なくとも電子メール手段及び閲覧表示手段を有する登録ユーザの通信端末と、
少なくとも個人識別情報と上記登録ユーザの電子メールアドレスを対応させた個人情報を保管し、ネットワークを介して受信した個人識別情報に基づいて個人認証を行なう請求項１～６のいずれかに記載の認証装置と
を備え、
上記登録ユーザの通信端末は、受信したロック通知メールに記載された上記ロック解除情報の通信アドレス先にアクセスして、上記ロック解除用識別情報を上記認証装置に与えて、個人識別情報の禁止を解除させることを特徴とする認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】

本発明は、認証装置及び認証システムに関し、例えば、ユーザ端末等から指示したコンテンツ情報（ファイル情報）を、コンビニエンスストアや駅などに設置されているマルチメディアキオスク端末（ＭＭＫ）等をユーザが利用して取得し印刷出力するＷｅｂを使用したサービスシステムにおいて、登録ユーザの個人認証を行なう認証装置及び認証システムに適用できる。

【０００２】

【従来の技術】

近年、インターネットの利用態様の多様化及び携帯電話等の移動通信端末の多機能化に伴い、インターネットを利用した様々なＷｅｂを使用したサービスがある。

【０００３】

例えば、ユーザが所持するブラウザ機能を搭載した携帯端末を利用してインターネット上のサーバと通信を行ない所望チケット等を予約購入するシステムについて記載されている（下記特許文献１参照）。また例えば、ユーザ又はその関係者がＷｅｂサーバにファイル情報の格納を行ない、ユーザがＭＭＫ等を利用して外出先からでもそのＷｅｂサーバのファイル情報を呼出し印刷出力するシステムサービスもある。

【０００４】

このような様々なＷｅｂを使用したサービスをユーザに提供する場合、そのユーザが本人であるか否かの正当性を判断することは重要であり、さまざまな認証方式がある（下記特許文献２参照）。

【０００５】

一般的な個人認証方式として、例えば、ユーザに割り当てられたユーザＩＤと本人しか知らないパスワード等の認証情報を認証装置のデータベースに予め登録しておき、ユーザがサービスを受ける際に、ユーザが移動通信端末やＭＭＫ等を利用してユーザＩＤ及びパスワードを入力して認証装置に送信し、受信した入力ユーザＩＤに基づいて、入力パスワードと登録パスワードとの一致・不一致を認証装置が判断することによりユーザの本人認証が行われている。

【０００６】

そして、認証装置が、ユーザＩＤ及びパスワードの一致と判断した場合、ユーザ本人の正当性を認め、不一致と判断した場合、ユーザ本人ではないと判断する。

【０００７】

【特許文献１】

特開２００２－２１５９８６号公報

【０００８】

【特許文献２】

特開２００２－２５９２６４号公報

【０００９】

【発明が解決しようとする課題】

しかしながら、ユーザはサービスを受けるためのユーザＩＤ及びパスワードを覚えておく必要があり、ユーザがユーザＩＤ及びパスワードを忘れてしまい、何度か連続して間違えたユーザＩＤ及びパスワード等を入力試行したにもかかわらず個人認証の正当性が得られなかった場合、認証装置はそのユーザＩＤを使用禁止にする場合がある。Ｗｅｂサーバが認証装置と連携する場合には、Ｗｅｂサーバによるサービスの提供も行われなくなる。

【００１０】

このような場合には、ユーザは、認証装置の運営者側又はサービス提供者側と直接連絡を取り、新たなユーザＩＤ等の発行や登録変更等のユーザＩＤの使用禁止状態を解除する所定の手続が必要であった。

【００１１】

また、このようなユーザＩＤの使用禁止状態を解除する手順を熟知している第三者は、あるユーザの入力ユーザＩＤ及び入力パスワードとして適当なものを入力して、ユーザＩＤを故意に使用禁止状態にした後に、認証装置運営者側又はサービス提供者と連絡を取り、

新しいユーザＩＤを取得することで、ユーザになりすましてサービスの提供を受けるというなりすまし行為が行われるおそれもある。

【００１２】

そのため、登録ユーザでないとの認証結果によりサービスが使用禁止状態になった場合に、そのサービス使用禁止状態の解除手続を、登録ユーザにとって利便性が高く、かつ、第三者によるなりすましを防止しより高いセキュリティで行なう認証装置及び認証システムが求められている。

【００１３】

【課題を解決するための手段】

かかる課題を解決するために、第１の本発明の認証装置は、（１）登録ユーザの各個人識別情報に、少なくとも各登録ユーザのユーザ通信端末の電子メールアドレスを対応付けた個人情報を記憶する個人情報記憶手段と、（２）登録ユーザの個人認証を行なう個人認証手段と、（３）個人認証手段により個人認証の正当性が認められず、個人識別情報が使用禁止とされたときに、当該個人識別情報の禁止を個別に解除するロック解除情報を作成するロック解除情報作成手段と、（４）使用禁止となった個人識別情報に対応する電子メールアドレスを送信先とし、少なくとも、ロック解除情報に割り当てた通信アドレスと、ロック解除用識別情報とを記載したロック通知メールを送信する電子メール通信手段と、（５）ロック解除情報に割り当てた通信アドレスにアクセスを受け、受信したロック解除用識別情報に基づいて認証を行ない正当である場合、使用禁止された個人識別情報の禁止を解除するロック解除手段とを備えることを特徴とする。

【００１４】

第２の本発明の認証システムは、（１）少なくとも電子メール手段及び閲覧表示手段を有する登録ユーザの通信端末と、（２）少なくとも個人識別情報と登録ユーザの電子メールアドレスを対応させた個人情報を保管し、ネットワークを介して受信した個人識別情報に基づいて個人認証を行なう第１の本発明の認証装置とを備え、登録ユーザの通信端末は、受信したロック通知メールに記載されたロック解除情報の通信アドレス先にアクセスして、ロック解除用識別情報を認証装置に与えて、個人識別情報の禁止を解除させることを特徴とする。

【００１５】

【発明の実施の形態】

（Ａ）実施形態

以下、本発明の認証装置及び認証システムの実施形態について図面を参照して説明する。

【００１６】

本実施形態は、ユーザ端末等から指示されたファイル情報をプリント管理サーバに格納させ、登録ユーザが、外出先からでもコンビニエンスストアや駅などに設置されているマルチメディアキオスク端末（ＭＭＫ）等を利用して、プリント管理サーバにアクセスしてファイル情報を取得し印刷出力するＷｅｂを使用したシステムに適用した場合を説明する。

【００１７】

（Ａ－１）実施形態の構成

図１は、本実施形態の認証システムの全体構成を示すものである。図１に示すように、本実施形態の認証システム１は、プリント管理サーバ２、認証情報データベース３、携帯電話４、プリント情報管理データベース５、コンビニエンスストア等に設置されている通信端末（ＭＭＫ）６、プリンタ８、ファイル登録を指示する通信端末９を備える。また、ネットワーク７は、公衆網や移動通信網やインターネット等の通信網であり、プリント管理サーバ２と、通信端末６と、携帯端末４と、ファイル登録を指示する通信端末９はネットワーク７を通じて接続可能である。

【００１８】

通信端末９は、プリント管理サーバ２にファイル情報の格納指示を行なう通信端末であり、ネットワーク７に接続可能なＰＣやブラウザ機能を有する携帯電話やＭＭＫ等が該当する。

【００１９】
プリント管理サーバ２は、通信端末９から登録指示されたファイル情報を、ユーザ毎に割り当てた保管領域に保管するものである。また、プリント管理サーバ２は、通信端末６からの印刷実行時により、保管しているファイル情報を通信端末６に送信するものである。なお、本実施形態では印刷実行する通信端末９をＭＭＫとして説明するが、プリンタデバイスと接続する通信端末であれば広く適用できる。
【００２０】
プリント管理サーバ２は、上記のほかに登録ユーザの個人認証処理、ユーザ管理、セキュリティ管理、印刷履歴管理、ファイル情報の印刷等に対する課金管理などを統合的に行なうサーバであり、コンテンツ情報の印刷サービスの提供をするものである。
【００２１】
プリンタ管理サーバ２は、認証処理時は、印刷実行時に通信端末６からのユーザＩＤ及びパスワードに基づいて認証処理を行なうものである。
【００２２】
プリント管理サーバ２は、ファイル情報の登録時に、ユーザの個人認証処理を行なわず、プリント管理サーバ２が発行したアドレスに対して、例えば、通信端末９からファイル情報を添付した電子メールを送信することで、アドレス（保管領域）にファイル情報を登録することができる。
【００２３】
また、プリント管理サーバ２は、プリント情報管理データベース５におけるファイル情報の格納位置情報と、登録ユーザによりファイル情報を呼出すための印刷識別情報とをユーザＩＤに対応させて管理し、外部から受信した印刷識別情報や個人識別情報に基づいて格納されたファイル情報や個人情報をネットワーク７を通じて送信するものである。
【００２４】
プリント情報管理データベース５は、登録ユーザにより指示されたファイル情報を格納するデータベースである。
【００２５】
次に、プリント管理サーバ２の個人認証部２ａについて、図２を参照して説明する。
【００２６】
図２に示すように、個人認証機能２ａは、制御部２１が実行するソフトウェアで構成され、通信部２２と、ユーザ登録機能部２３と、個人認証機能部２４と、ロック解除機能部２５とを有する。
【００２７】
制御部２１は、プリント管理サーバ２の個人認証機能を制御するものである。
【００２８】
ユーザ登録機能部２３は、Ｗｅｂを使用したサービスの提供を受けるユーザの個人情報を認証情報データベース３に登録・保存し、図３に示す認証情報管理テーブルを有して登録ユーザの認証情報を管理するものである。
【００２９】
認証情報管理テーブルは、図３に示すように、プリント管理サーバ２側が各登録ユーザを識別するために付与したユーザＩＤに、少なくとも、サーバあるいはユーザが決定したパスワード（例えば、最初はサーバ側が決定したパスワードを発行し、その後ユーザにより決定できるパスワードを含む）、電子メールアドレス、所定の監視期間内に発生した総ロック回数、ロック発生時に付与されるロックフラグを対応させ記憶するものである。勿論、他の項目として、ユーザの氏名・住所、電話番号や年齢その他の個人情報、認証履歴等を記憶するようにしてもよい。
【００３０】
ここで、電子メールアドレスは、登録ユーザ本人に電子メールを送信するために必要であり、ユーザが所持する電子メール機能を有する携帯電話４の電子メールアドレスや、ユーザが所有するＰＣの電子メールアドレス等を示す。本実施形態ではユーザが所持する携帯

電話４の電子メールアドレスとする。

【００３１】

また、登録するパスワードや電子メールアドレスの数を複数個としても良い。また、ユーザ登録機能部２３は、登録ユーザの意思に基づいて、認証情報データベース３に保存した個人情報の内容を変更・追加・削除できるようにしてもよい。この場合、既に登録されているユーザＩＤ及びパスワードによる個人認証処理後に行なうことが好ましい。

【００３２】

例えば、ユーザの電子メールアドレスを変更する場合、登録ユーザの個人認証の正当性を判断した後、ユーザ登録機能部２３は、登録ユーザの操作による通信端末９からのユーザＩＤに対応する個人情報を認証情報データベース３から取り出し、新しい電子メールアドレスに上書き修正したり、又は、登録電子メールアドレスを削除して新しい電子メールアドレスを再登録する等して変更できるようにしてよい。また、個人情報の内容の追加についても、個人情報の内容の変更と同様にしてするようにしてよい。また、個人情報の内容の削除は、個人情報の一部又は全部を削除するようにしてもよい。

【００３３】

個人認証機能部２４は、Ｗｅｂを使用したサービスの提供前に、Ｗｅｂを使用したサービスの利用希望者にユーザＩＤ及びパスワードの入力要求後、その入力ユーザＩＤ及びパスワードに基づいて、ユーザの個人認証を行なうものである。

【００３４】

個人認証機能部２４は、受信したユーザＩＤに基づいて認証情報データベース３に登録されている個人情報を取り出し、その対応する登録パスワードと入力パスワードとが一致するか否かを判断して認証するものであり、入力パスワードと登録パスワードとが一致する場合、登録ユーザ本人であることを認め、また入力パスワードと登録パスワードとが不一致である場合、登録ユーザ本人でないと判断する。

【００３５】

個人認証がＮＧの場合、個人認証機能部２４は、通信端末９に対して所定回数（例えば３回）の再試行の機会を要求してもよい。また、この再試行によっても個人認証がＮＧである場合は、登録ユーザでないと判断し、そのユーザＩＤを使用不可能な状態に（ロック）する。ユーザＩＤのロックは、例えば、そのユーザＩＤに対応する個人情報にロックした旨のフラグをたてて、フラグがたててあるユーザＩＤについては使用不可能であるものとし、認証情報データベース３に保存するようにする。

【００３６】

また、個人認証機能部２４は、ロックされたユーザＩＤに対応する個人情報から総ロック回数を監視し、総ロック回数が所定の監視期間内で所定回数（例えば３回）以上である場合、新たなユーザＩＤを準備（確保）する。

【００３７】

個人認証機能部２４は、登録されているユーザＩＤを新しいユーザＩＤに変更し、既に登録されているユーザの個人情報を新しいユーザＩＤに対応させて認証情報データベース３に保存する。

【００３８】

この総ロック回数の監視期間及び総ロック回数は、認証装置２の管理者側が、例えば、時分、日、月、年等の単位で自由に設定できる。また、登録ユーザが、登録時又は登録後に、この監視期間及び総ロック回数を指定できるようにしてもよい。

【００３９】

ロック解除機能部２５は、個人認証機能部２４によりユーザＩＤがロックされると、そのロックされたユーザＩＤのロックを解除するためのファイル情報を作成し、そのファイル情報をロック解除用サイトとしたＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を作成する。

【００４０】

このロック解除用サイトは、ユーザＩＤのロック発生につき、そのユーザＩＤに対応する

ＵＲＬが割り当てられて作成されるものであって、そのＵＲＬは、他のロック解除用サイトのＵＲＬと同時期に重複しないものである。ロック解除用サイトは、例えば、１個のユーザＩＤに対応する１個のＵＲＬを発行し、その後のユーザＩＤのロック発生後にも、同一のＵＲＬを使用させることができる。また、各ロック発生毎に異なるＵＲＬを作成させるようにしてもよい。

【００４１】

また、ロック解除機能部２５は、ロック解除サイト作成後、ロックされたユーザＩＤに対応する電子メールアドレスを送信先として、ロック解除用サイトのＵＲＬと、ユーザＩＤ及びパスワードとをメール内容に記載した電子メール（ロック通知メール）を送信する。登録された電子メールアドレスにロック通知メールを送信することで、正確に登録ユーザに通知することができる。

【００４２】

なお、ロック通知メールに、プリント管理サーバ２の管理者側の電話番号やユーザＩＤのロック発生の年月日時等やその他情報も記載するようにしてもよい。

【００４３】

ロック解除機能部２５は、ユーザＩＤのロック解除が終了すると、割り当てられたＵＲＬを無効にする。

【００４４】

ロック解除機能部２４は、ロックされたユーザＩＤについてのロック解除が終了すると、ロック通知メールを送信した送信先と同様の電子メールアドレス（登録ユーザの登録電子メールアドレス）に、ロックが解除された旨のロック解除通知メールを送信する。

【００４５】

ロック解除用サイトでは、ロック通知メールを携帯電話４で受信したユーザが利用する通信端末（例えばＭＭＫ６、ユーザの通信端末９等を含む）から、電子メールに記載のＵＲＬに基づいてアクセスされ、電子メールに記載のユーザＩＤ及びパスワードの入力送信要求をその通信端末に行なう。ロック解除用サイトでは、受信したパスワードと登録パスワードとの一致・不一致を判断して、一致する場合には、そのユーザＩＤのロックを解除し、不一致の場合にはユーザＩＤのロックを維持する。不一致の場合には、所定回数の再試行を要求してもよい。また、ユーザは、可能であれば、ブラウザ機能を有する携帯電話２からロック解除用サイトにアクセスできるようにしてもよい。

【００４６】

通信部２２は、通信ボードや通信ソフトウェア等が該当し、ネットワーク７の通信を可能にする通信機能及び電子メール通信機能を有するものである。

【００４７】

図１に戻り、通信端末６は、コンビニエンスストアや駅などに設置されているマルチメディアキオスク端末等が該当し、図６に示すように、ユーザ操作部６１、情報通信部６２、画面表示部６３、一時的に情報を記憶する記憶部６４、制御部６５、プリンタ制御部６６などを有するものである。

【００４８】

また、通信端末６は、ユーザの操作により、ネットワーク７を通じてプリント管理サーバ２からファイル情報を取得し、接続するプリンタ８からファイル情報を出力するものである。

【００４９】

携帯電話２は、Ｗｅｂブラウザ機能及び電子メール機能を有する携帯電話であり、ユーザの操作により、認証装置２とアクセスし得るものである。携帯電話４は、Ｗｅｂブラウザ機能により、認証装置２が有するコンテンツを閲覧可能であり、認証装置２からの要求に応じてユーザＩＤ及びパスワード等の入力及び送信するものである。また、携帯電話４は、電子メール機能により、認証装置２から電子メールを受信可能であり、その電子メールに添付されたロック解除用サイトのＵＲＬをユーザに知らせるためのものである。

【００５０】

（Ａ－２）実施形態の動作
次に、本実施形態の認証装置及び認証システムの動作について説明する。
【００５１】
以下では、プリント管理サーバ２による個人認証部２ａの個人認証処理、ユーザＩＤのロック動作及びロックされたユーザＩＤのロック解除動作について詳細に説明する。
【００５２】
なお、登録ユーザのユーザＩＤ、パスワード及び電子メールアドレスを少なくとも含む個人情報は、認証情報データベース３に予め登録されていることを前提として説明する（Ｓ１）。
【００５３】
まず、プリント管理サーバ２のサービスの提供を受けようとする者（保管ファイル情報の印刷実行する者）の操作により、通信端末（ＭＭＫ）６はプリント管理サーバ２の個人認証部２ａにアクセスする（Ｓ２）。なお、以下では、プリント管理サーバ２へのアクセスを通信端末（ＭＭＫ）６によるものとして説明するが、これに限らずユーザがサービス利用を行なう際に利用する通信端末（例えば図１の通信端末９）であれば広く適用できる。
【００５４】
通信端末（ＭＭＫ）６において、ユーザＩＤ及びパスワードが、希望者の操作により入力され、入力されたユーザＩＤ及びパスワードが通信端末（ＭＭＫ）６から個人認証部２ａに送信される（Ｓ３）。
【００５５】
通信端末（ＭＭＫ）６からのユーザＩＤ及びパスワードは個人認証部２ａに受信され（Ｓ４）、個人認証部２ａにおいて、受信したユーザＩＤに対応するユーザのパスワードが認証情報データベース３から取り出され、受信したパスワードと登録されているパスワードとの一致・不一致が判断される（Ｓ５）。
【００５６】
パスワードが一致する場合、ユーザが登録ユーザ本人であるとして認証動作を終了し（Ｓ６）、プリント管理サーバ２のサービスを受けることが可能となる。
【００５７】
個人認証がＮＧの場合、ユーザＩＤ及びパスワードの連続試行回数を検知し（Ｓ７）、その試行回数が所定回数未満である場合には、通信端末（ＭＭＫ）６に対して、ユーザＩＤ及びパスワードの再試行入力を通信端末（ＭＭＫ）６に要求する（Ｓ８）。
【００５８】
この再試行入力要求に応じて、希望者の操作により、通信端末（ＭＭＫ）６からの再度ユーザＩＤ及びパスワードの入力・送信が行われ、上述したＳ３～Ｓ７の動作が繰り返される。
【００５９】
個人認証部２ａにより検知された試行回数が所定回数以上である場合、当該ユーザＩＤが使用不可能に（ロック）される（Ｓ９）。
【００６０】
ユーザＩＤをロックする方法として、例えば、そのユーザＩＤに対応する個人情報のうち、ロックしたことを示すフラグをたてて、このフラグがあるユーザＩＤについては使用不可能とするように、認証情報データベース３に保存する。
【００６１】
また、個人認証部２ａにより、ロックがある毎にユーザＩＤに対応する個人情報のうち総ロック回数が更新される（Ｓ１０）。ここで、総ロック回数が所定監視期間内に所定回数未満であると個人認証部２ａが判断した場合、総ロック回数をクリアしてもよい。
【００６２】
個人認証部２ａにおいて、総ロック回数が監視され（Ｓ１１）、所定監視期間内の総ロック回数が所定回数（例えば３回）以上であると判断された場合、当該ユーザＩＤに代えて新しいユーザＩＤを発行するために、新しいユーザＩＤが準備される（Ｓ１２）。なお、

新しいユーザＩＤは、ユーザによるロック解除要求の後で発行されるようにしてもよいし、新しいユーザＩＤの発行をユーザに問い合わせ希望する場合にのみ発行されるようにしてもよい。

【００６３】

新しいユーザＩＤが準備された後、ロックされたユーザＩＤのロックを解除するためのロック解除用サイトが作成される（Ｓ１３）。

【００６４】

また、Ｓ１１に戻り、総ロック回数が所定回数未満であると判断された場合は、新しいユーザＩＤの準備はされずに、ロック解除用サイトが作成される（Ｓ１１及びＳ１３）。

【００６５】

このロック解除用サイトは、ユーザＩＤのロック発生につき、そのユーザＩＤに対応するＵＲＬが割り当てられて作成されるものであって、そのＵＲＬは、他のロック解除用サイトのＵＲＬと同時期に重複しないものである。

【００６６】

個人認証部２ａにより、認証情報データベース３からロックされたユーザＩＤに対応する個人情報が取り出され、登録されているユーザの電子メールアドレスを送信先として、今回のロックにつき作成されたロック解除用サイトのＵＲＬ、登録されているユーザＩＤ及びパスワードが、電子メール内容として記載されたロック通知メールが作成され送信される（Ｓ１４及びＳ１５）。登録された電子メールアドレスにロック通知メールを送信することにより、当該システム利用が、悪意ある第三者であっても、ロックの登録ユーザ本人にのみ通知できる。

【００６７】

ロック通知メールが送信された後は、ロック解除用サイトは、ユーザによる携帯電話４からのロック解除要求の受付けるべく待機状態となる（Ｓ１６）。

【００６８】

次に、ロック通知メールを受信したユーザの要求によりユーザＩＤのロックを解除する動作について図５を参照して説明する。

【００６９】

上述したように、個人認証部２ａは、ロック通知メールを送信後、ロック解除用サイトへのアクセスによるユーザのロック解除要求があるまで、ロック解除要求の待機状態となる（Ｓ２１）。

【００７０】

ユーザの操作により、ロック通知メールに記載のロック解除用サイトのＵＲＬにアクセスする（Ｓ２２）。この場合に、ユーザがロック解除用サイトにアクセスするための通信端末６は、ユーザが利用可能な通信端末であれば広く適用でき、例えば、通信端末９、通信端末（ＭＭＫ）６、ブラウザ機能を有する携帯電話４等を適用するようにしてもよい。

【００７１】

例えば、ユーザが外出時にロック通知メールを携帯電話４で受信した後、その受信した位置に近接する通信端末（ＭＭＫ）６を利用してロック解除用サイトにアクセスしたり、また例えば、会社内にいる場合には、会社でユーザが使用するパソコン（通信端末９）からアクセスするようにしてもよい。

【００７２】

なお、以下では、ユーザがロック解除用サイトにアクセスする通信端末を通信端末（ＭＭＫ）６として説明する。

【００７３】

ロック解除用サイトにアクセスした後、ユーザに対しロック通知メールに記載のユーザＩＤ及びパスワードを入力するよう要求し、この要求に応じて、ユーザの操作により、ユーザが利用した通信端末６からロック通知メールに記載のユーザＩＤ及びパスワードが入力され個人認証部２ａのロック解除用サイトに送信される（Ｓ２３）。このとき、ユーザの意思により、ユーザの個人情報（例えばパスワード等）の変更を個人認証部２ａが受け付

けるようにしてもよい。
【００７４】
個人認証部２ａのロック解除用サイトにおいて、ユーザが利用した通信端末６からのユーザＩＤ及びパスワードを受信し（Ｓ２４）、ロック解除用サイトに対応付けられたユーザＩＤ及びパスワードが正しいか否かが判断される（Ｓ２５）。
【００７５】
ロック解除用サイトによりユーザＩＤ及びパスワードが正しくないと判断された場合、そのまま当該ユーザＩＤのロックは維持される（Ｓ２６）。このとき、ユーザＩＤ及びパスワードの入力について所定回数の再試行を要求できるようにしてもよい。
【００７６】
ロック解除用サイトによりユーザＩＤ及びパスワードが正しいと判断された場合、個人認証部２ａが準備する新しいユーザＩＤが存在するか否かを確認する（Ｓ２７）。
【００７７】
これは、ロックされたユーザＩＤについて、新しいユーザＩＤを発行して登録するのか否かを確認するためである。
【００７８】
勿論、新しいユーザＩＤをユーザのロック解除要求の後で発行する場合には、ロック解除用サイトによるユーザＩＤ及びパスワードの認証後又はユーザのユーザＩＤの発行要求後、新しいユーザＩＤの発行動作が加わり、新しいユーザＩＤの存在確認動作は行われない。
【００７９】
個人認証部２ａにおいて、新しいユーザＩＤが準備されている場合には、新しいユーザＩＤとユーザの個人情報とを対応させて認証情報データベース３に保存し、新しいユーザＩＤの有効性を確保する（Ｓ２８）。
【００８０】
このとき、ロックされたユーザＩＤ及びそのユーザＩＤに対応させた個人情報を削除するようにしてもよいし、又はこのユーザＩＤの使用不可能な情報にしたまま認証情報データベース３に保持するようにしてもよい。
【００８１】
新しいユーザＩＤの発行後、ユーザの個人情報を対応させた新しいユーザＩＤを認証情報データベース３に登録することで、新しいユーザＩＤを有効にしロックを解除する（Ｓ２９）。
【００８２】
Ｓ２７に戻り、新しいユーザＩＤが準備されていない場合には、ロックされたユーザＩＤに対応する個人情報のフラグを削除することでロックを解除する（Ｓ２７及びＳ２９）。
【００８３】
ユーザＩＤのロック解除終了後、当該ロック発生時に作成したロック解除用サイトのＵＲＬを無効にする（Ｓ３０）。ロック解除用サイトのＵＲＬを無効にする時期は、これに限られず、例えば、ロック解除通知メールをユーザの携帯電話４に送信後に無効にしてもよい。
【００８４】
ユーザＩＤのロック解除終了後、当該ユーザＩＤに対応するユーザの電子メールアドレスを送信先として、ロック解除が終了した旨のロック解除通知メールを作成し、送信する（Ｓ３１及びＳ３２）。
【００８５】
個人認証部２ａからロック解除通知メールを受信したユーザは、ユーザＩＤのロックが解除した旨を知り、既存のユーザＩＤ又は新しいユーザＩＤを用いることで個人認証を行なうことができる（Ｓ３３）。
【００８６】
（Ａ－３）実施形態の効果

以上、本実施形態によれば、認証処理時に、少なくともユーザのみが知るパスワード及びユーザの電子ールアドレスを予め登録し、ユーザＩＤのロック発生時に、ユーザの電子メールアドレスを送信先として、ロック解除用サイトのＵＲＬ、ユーザＩＤ及びパスワードを記載した電子メールを送信することで、登録したユーザにのみ正確にユーザＩＤのロックの旨及びユーザＩＤ及びパスワードの確認をさせることができると共に、登録したユーザのみの操作により、ロック解除用サイトにアクセスしユーザＩＤのロック解除処理を行なわせることができる。その結果、第三者によるなりすましを防止することができる。

【００８７】

また、本実施形態によれば、ユーザにとって負担が少ないロック解除処理でロック解除を行なわせることができる。

【００８８】

（Ｂ）他の実施形態

（Ｂ－１）上述した実施形態では、ユーザが所持する携帯電話を利用して個人認証する場合について説明したが、携帯電話に限らず、ＰＤＡやＰＨＳ等その他の移動通信端末やパソコンや店舗に設置されたＭＭＫ等の通信端末等広く適用できる。

【００８９】

また、携帯端末４に与えられたロック通知メール及びロック解除通知メールを、通信端末（ＭＭＫ）６に転送できるようにしてもよい。このとき、個人認証部２ａは、携帯端末４の位置情報（例えば基地局５から割り出した情報やＧＰＳを利用した緯度経度情報等）を確認し、その位置情報周辺の１又は複数の通信端末（ＭＭＫ）６を特定し、その特定した公共通信端末（ＭＭＫ）６でのみ転送指定できるようにしてもよい。

【００９０】

また、ユーザにＷｅｂを使用したサービスを提供するＷｅｂサーバ又はシステムが、上述した認証装置及び認証システムを利用することができる。このとき、上述した認証装置及び認証システムは、Ｗｅｂサーバ又はシステム自身が含む装置としてよいし、又はＷｅｂサーバ又はシステムとは異なる装置としてもよい。

【００９１】

（Ｂ－２）上述した実施形態において、ロック解除用サイトによるユーザＩＤのロック解除は、ロック通知メールに記載のユーザＩＤ及びパスワードの認証により行なうこととして説明したが、これに限らず、例えば、ロック解除機能部２５が発行したロック解除用キーをロック通知メールに添付し、ロック解除キーのユーザ入力に基づいてロック解除できるようにしてもよい。

【００９２】

この場合、ロック解除用キーの発行は、ロック解除用サイトの作成時に、ロック解除機能部２５が発行し、当該ユーザＩＤとロック解除用キーとを対応させて保存することにより認証するようにする。

【００９３】

また、ロック通知メールにユーザＩＤ及びパスワードを記載することとしたが、ユーザの個人情報登録時に、これらユーザＩＤ及びパスワードをロック通知メールに記載するか否か、又は、ロック通知メールに記載する内容をユーザに選択できるようにしてもよい。

【００９４】

（Ｂ－３）上述した個人認証部２ａは、図５のＳ２１～Ｓ２４でロック解除用サイトの解除要求の受付期限を設定するようにしてもよい。例えば、この解除要求の受付期限を、ロック通知メールの送信日から所定期間（例えば１週間、６ヶ月、１年等設定できる）内と設定し、その期間内にユーザからの解除要求がない場合には、ロックされたユーザＩＤのロック解除は行われないようにしてもよい。この場合、個人認証部２ａはロック解除用サイトのＵＲＬを無効にしたり、又は、当該ユーザＩＤに対応する個人情報を削除したりしてもよい。

【００９５】

（Ｂ－４）上述した実施形態の変形例として、ロック解除用サイトのＵＲＬを記載せず、

ロックした旨を記載した第１のロック通知メールをユーザの携帯電話４に送信し、まずユーザに電子メールの返信を求めるようにしてもよい。

【００９６】

そして、個人認証部２ａがユーザからの電子メール返信を確認した後に、ロック解除用サイトのＵＲＬを記載した第２のロック通知メールをユーザの携帯電話４に送信するようにしてもよい。

【００９７】

また、第１のロック通知メールに対して返信されたユーザの返信電子メールにより、ユーザがロック解除要求、及び又は、新しいユーザＩＤの発行要求をするようにしてもよい。

【００９８】

（Ｂ－５）また、上述した実施形態では、ロック発生したユーザＩＤ専用のロック解除サイトを作成することとしたが、これに限ることなく、ロック発生したユーザＩＤを所有する全てのユーザ共通のロック解除サイトを作成するようにしてもよい。

【００９９】

例えば、上記共通ロック解除サイトを認証装置２が有するホームページ上に表示し、ロック通知メールを受信したユーザが、上記ホームページ上の共通ロック解除サイトにアクセスして、自身のユーザＩＤのロック解除を行なうようにしてもよい。

【０１００】

この場合、ロック解除機能部２５が、ユーザＩＤのロック発生時に、当該ユーザＩＤ専用のロック解除用キーを発行し、そのロック解除用キーをロック通知メールに添付してユーザに送信する。そして、ユーザからの解除要求の際に、ユーザ入力されたロック解除用キーに基づいて、ロック解除用サイトが認証するようにしてもよい。

【０１０１】

【発明の効果】

以上、本発明によれば、登録ユーザのみがロック通知メールを受信することができ、ロック通知メールを受信した登録ユーザのみが個人識別情報のロックを容易に解除することができる。その結果、第三者による成りすましを防止することができる。

【図面の簡単な説明】

【図１】実施形態の認証システムの全体構成を示す図である。

【図２】実施形態の認証装置２の機能構成を示す図である。

【図３】実施形態の認証情報データベース３が保存する認証情報の項目例を示す説明図である。

【図４】実施形態の認証装置２の動作を説明するフローチャートである。

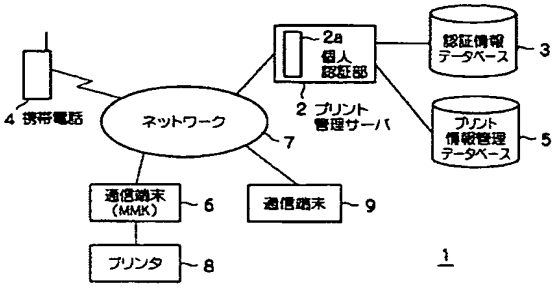
【図５】実施形態の認証装置２の動作を説明するフローチャートである。

【図６】実施形態の通信端末６の内部構成を示す図である。

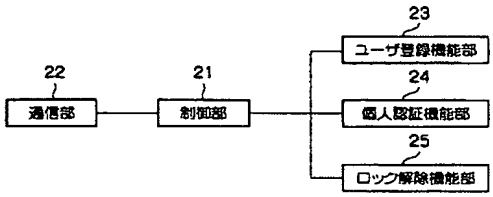
【符号の説明】

１…認証システム、２…プリント管理サーバ、２ａ…個人認証部、
３…認証情報データベース、４…携帯電話、２１…制御部、２２…通信部、
２３…ユーザ登録機能部、２４…個人認証機能部、２５…ロック解除機能部。

【図１】



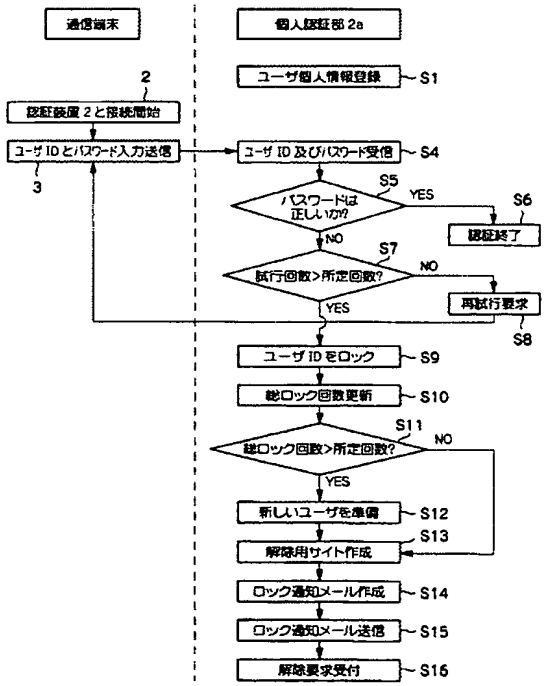
【図２】



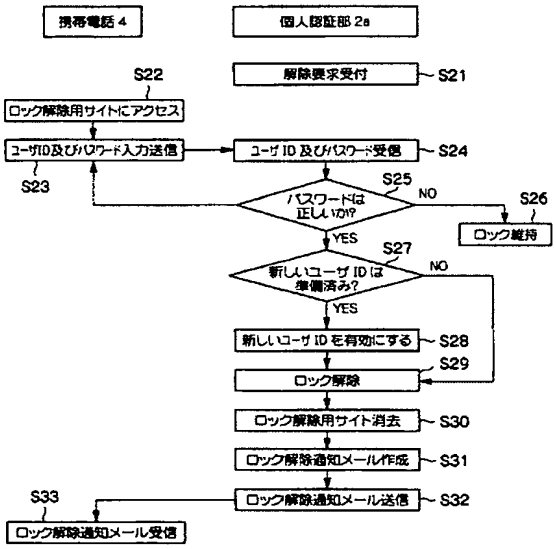
【図３】

ユーザID	パスワード	電子メールアドレス	総ロック回数	ロックフラグ
101011	yamamoto	yama@XXXX.XXX	3	✓
101013	kawa0102	kawa@△△△.***		
...	...			

【図４】



【図５】



【図６】